The second and third columns are the command line parameters to use to read from and write to a pcap file insteand of an interface, respectively.

Applications					
Application	**R**	**W**	**OS**	**URL**	**Last**
ADMsniff	n/a			http://packetstormsecurity.nl/groups/ADM/	1998
AimSniff	−r	n/a		http://sourceforge.net/projects/aimsniff/	2003
AIM Sniff is a network sniffer specifically designed to pick up messages transmitted using the AOL Instant Messenger client and its derivatives. All information can be sent to STDOUT or a MySQL DB.					
AirSnort				http://airsnort.shmoo.com/	2003
AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.					
Aldebaran	n/a	−f		http://www.rogala.3d.pl/en/aldebaran.htm	2001
Aldebaran is an advanced libpcap−based network TCP sniffer. It gives a user only a payload from captured data and basic info about addresses and ports (nothing about flags, etc.). This is useful for monitoring data sent by connections and sniffing passwords. It supports filtering packets with not only simple port/address libpcap rules but also payload contents and can send captured data to another host via UDP.					
Altivore				http://www.robertgraham.com/altivore/ http://downloads.securityfocus.com/tools/altivore.c	2000
This is a sample program containing some of the features of the features of the FBI's "Carnivore" program. It is intended to serve as a point of discussion about Carnivore features. It has not been thoroughly tested and contains numerous bugs.					
Analyzer				http://analyzer.polito.it/	2003
Analyzer is a full configurable network analyzer program for Win32 environment. Analyzer is able to capture packets on all platforms (and link−layer technologies) supported by WinPcap, except for Windows 95.					
Angst	n/a			http://angst.sourceforge.net/	2001
Angst is an active sniffer, based on libpcap and libnet. Angst provides methods for aggressive sniffing on switched local area network environments. It dumps the payload of all the TCP packets received on the specified ports. Moreover, it implements methods for active sniffing.					
Antisniff	n/a			http://packetstormsecurity.nl/sniffers/antisniff/	2000
Antisniff, originally by l0pht but now discontinued, may be able to detect some sniffers running on the local network.					
Aps	n/a			http://www.swrtec.de/clinux/	2001
APS − Advanced Packet Sniffer − tries to print detailed info about network frames that are received from the SOCK_RAW (ETH_P_ALL) socket (maybe this will get to libpcap in any future release, at least i hope so !! :−) . APS prints info about the hardware layer and the IP and TCP/UDP/ICMP header. The tail of the packet (mostly the data) wich could not be interpreted is written on the screen as ascii/hex−dump or both.					
Apsr				http://www.aa−security.de/	2003

APSR is a network testing tool, designed to send and recieve arbitrary network packets. It can be used to test firewalls, routing, security and many other things. The project is split in two main programs, apsend to create packets and aprecv to sniff packets.				
Argus			http://www.qosient.com/argus/	2003
Argus is a fixed−model Real Time Flow Monitor designed to track and report on the status and performance of all network transactions seen in a data network traffic stream.				
ARP0c	n/a		http://www.phenoelit.de/arpoc/	2001
ARP0c is a connection interceptor (using ARP spoofing and a bridging engine). ARP requests from various sources in a switched environment get false ARP response packets which point to the host running ARP0c. Packets from these hosts are bridged with an internal engine to the real destination address to allow normal network operation and keep TCP connections alive.				
Arpscan		? 	http://ish.cx/~jason/arpscan/	2003
Arpscan is a very simple scanner which sends out arp requests for the given IP addresses and displays a list of the found hosts.				
Arpwatch			http://www.tcpdump.org	2001
Arpwatch and arpsnmp are both network monitoring tools. Both utilities monitor Ethernet or FDDI network traffic and build databases of Ethernet/IP address pairs, and can report certain changes via email.				
Bro			http://www.icir.org/vern/bro.html	2003
Bro is an intrusion detection system that works by passively watching traffic seen on a network link.				
Buttsniff			http://packetstormsecurity.nl/sniffers/buttsniffer/	2000
Standalone packet sniffer for Windows or back oriface sniffer plugin.				
Cain and Abel			http://www.oxid.it/cain.html	2003
Cain &Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary &Brute−Force attacks, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols.				
Carnivore				
cdpr			http://www.monkeymental.com/nuke/	2003
cdpr decodes a Cisco Discovery Protocol packet, and will by default show you the switch, it's IP address, and what port you are connected to. Optionally it will decode an entire CDP packet.				
Clog	−o		ftp://coast.cs.purdue.edu/pub/tools/unix/logutils/clog/	1997
Clog is a sniffer that can detect stealth scanners and ftp bounce attacks.				
Cold			http://www.ipv4.it/cold/	2003
A network analysis tool and protocol sniffer.				
Confuse Router			http://pedram.redhive.com/projects.php	2001
A tool I wrote to allow me to sniff partial traffic in a switched environment where arp requests/replies are not broadcasted to every node (ie: cable modem).				

Courtney	n/a			ftp://coast.cs.purdue.edu/pub/tools/unix/logutils/courtney/	1995
Courtney monitors the network and identifies the source machines of SATAN probes/attacks.					
Cutter				http://www.lowth.com/cutter/	2003
Cutter is an open source program that uses the FIN−ACK−RST packet technique to abort TCP/IP connections routed over the firewall or router on which it is run.					
Darkstat				http://members.optushome.com.au/emikulic/net/darkstat/	2003
darkstat is a network traffic analyzer. It's basically a packet sniffer which runs as a background process on a cable/DSL router and gathers all sorts of useless but interesting statistics.					
Despoof	n/a			http://razor.bindview.com/tools/	2000
Despoof is a free, open source tool that measures the TTL to determine if a packet has been spoofed or not.					
dhcp−agent		? 		http://www.whitefang.com/dhcp−agent/	2003
dhcp−agent is a portable UNIX Dynamic Host Configuration suite.					
Dice				http://www.ngthomas.co.uk/dice.htm	2003
Dice is a Windows program for decoding sniffer files.					
DNS Hijacker	n/a			http://pedram.redhive.com/projects.php	2002
dnshijacker is a libnet/libpcap based packet sniffer &spoofer. a versatile tool, dnshijacker supports tcpdump style filters that allow you to specifically target victims. dns answers are forged based on entries in a "fabrication table" or by simply forging one answer to all requests. a print only mode is also supported, allowing one to simply monitor dns traffic.					
dnstop	*	n/a		http://dnstop.measurement−factory.com/	2003
dnstop is a libpcap application (ala tcpdump) that displays various tables of DNS traffic on your network, including tables of source and destination IP addresses, query types, top level domains and second level domains. (* File to read is the last parameter on the command line)					
Driftnet				http://www.ex−parrot.com/~chris/driftnet/	2002
Driftnet is a program which listens to network traffic and picks out images from TCP streams it observes. In an experimental enhancement, driftnet now picks out MPEG audio streams from network traffic and tries to play them.					
dsniff	−r	−w		http://www.monkey.org/~dugsong/dsniff/	2002
dsniff was designed to audit networks and to demonstrate the insecurity of cleartext / weakly−encrypted network protocols and ad−hoc PKI.					
Egressor	n/a			http://www.packetfactory.net/projects/egressor/	2000
MITRE has released a freeware tool that allows a company to check the configuration of their Internet point−of−presence router. The tool will help companies determine whether their routers are configured to the Help Defeat Denial of Service Attacks guidelines. This configuration of egress filtering reduces the chance that their computers can unwittingly contribute to a distributed denial of service attack.					
etherape	−r	n/a		http://etherape.sourceforge.net/	2003

EtherApe is a graphical network monitor for Unix modeled after etherman. Featuring link layer, ip and TCP modes, it displays network activity graphically. Hosts and links change in size with traffic. Color coded protocols display. It supports Ethernet, FDDI, Token Ring, ISDN, PPP and SLIP devices. It can filter traffic to be shown, and can read traffic from a file as well as live from the network.					
ethereal / tethereal	−r	−w		http://www.ethereal.com/	2003
Ethereal is a network traffic analyzer for Unix−ish operating systems. Ethereal is the graphical display program, tethereal is suitable for command line usage.					
Etherpeek				http://www.wildpackets.com/products/etherpeek_mac http://www.wildpackets.com/products/etherpeek	2002
EtherPeek is an award−winning Ethernet network traffic and protocol analyzer designed to make the complex tasks of troubleshooting and debugging mixed−platform, multi−protocol networks easy.					
Etherscan Analyzer				http://www.etherscan.com/Products/Analyzer/	2003
Etherscan Analyzer is an advanced network traffic and protocol analyzer, which works in all Windows−based operating systems. With Etherscan, you can capture and analyze all packets transmitted in your segment of the local network. Etherscan decodes all major protocols, including Ethernet, NetBEUI, TCP/IP, and TCP/IP utilities. It is capable of reconstructing TCP/IP sessions.					
Etherscan password sniffer				http://www.etherscan.com/Products/Password/	2003
Etherscan Password Sniffer is a network sniffer program designed to capture and reveal passwords from many well−known protocols such as ftp, http, icq, irc, pop3 and many others.					
Ethersniff				http://packetstormsecurity.nl/sniffers/ethersniff.c	2003
A simple utility to probe for the etherleak vulnerability discussed in the Atstake paper where multiple platforms have ethernet Network Interface Card (NIC) device drivers that incorrectly handle frame padding, allowing an attacker to view slices of previously transmitted packets or portions of kernel memory due to poor programming practices.					
ettercap	−T	−Y		http://ettercap.sourceforge.net/	2003
ettercap is a network sniffer/interceptor/logger for ethernet LANs (both switched or not). It supports active and passive dissection of many protocols (even ciphered ones, like SSH and HTTPS). Data injection in an established connection and filtering (substitute or drop a packet) on the fly is also possible, keeping the connection synchronized. Many sniffing modes were implemented to give you a powerful and complete sniffing suite. Plugins are supported. It has the ability to check whether you are in a switched LAN or not, and to use OS fingerprints (active or passive) to let you know the geometry of the LAN. The passive scan of the lan retrives infos about: hosts in the lan, open ports, services version, type of the host (gateway, router or simple host) and extimated distance in hop.					
Firewalk	n/a			http://www.packetfactory.net/projects/firewalk/	2002
Firewalk is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device will pass.					
Firewall Tunnel	n/a			http://www.employees.org/~hek2000/projects/firewallTunnel/	2002
Enable servers behind a firewall to export TCP and UDP services to the external networks with the assistance from an externel host as proxy.					
flow−tools libpcap patch				http://www.splintered.net/sw/flow−tools/ http://www.net.informatik.tu−muenchen.de/~robin/flowtools/	2003
Flow−tools is a software package for collecting and processing NetFlow data from Cisco and Juniper routers.					

flowprobe	n/a		http://sourceforge.net/projects/fprobe	2003
fprobe: a NetFlow probe − libpcap−based tool that collects network traffic data and emits it as NetFlow flows towards the specified collector.				
fprobe			http://psi.home.ro/flow/	2003
This is a small NetFlow probe which will listen on a interface using libpcap, aggregate the traffic and export NetFlow V5 datagram to a remote collector for processing. A flow is identified by ip protocol, source ip, source port, destination ip, destination port.				
Fragroute	n/a		http://www.monkey.org/~dugsong/fragroute/	2002
fragroute intercepts, modifies, and rewrites egress traffic destined for a specified host, implementing most of the attacks described in the Secure Networks "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection" paper of January 1998.				
fwmon	n/a	−t	 http://www.scaramanga.co.uk/fwmon/	2002
This program allows you to monitor ipchains/iptables output in realtime. It supports both logging to a file/stdout and/or to tcpdump format capture logs. It also supports security features such as running non−root, and chrooting itself.				
ganglia			http://ganglia.sourceforge.net/	2003
Ganglia is a scalable distributed monitoring system for high−performance computing systems such as clusters and Grids. It is based on a hierarchical design targeted at federations of clusters. It relies on a multicast−based listen/announce protocol to monitor state within clusters and uses a tree of point−to−point connections amongst representative cluster nodes to federate clusters and aggregate their state.				
GreedyDog			http://www.shadowpenguin.org/sc_toolbox/unix/gdd/	2002
GreedyDog is the ethernet packet sniffer for Linux, FreeBSD, OpenBSD, NetBSD, Solaris2, SunOS4, AIX, HP−UX, IRIX, MacOSX, and Windows2000/Xp. GreedyDog keeps stream of each TCP session and writes to logfile. So, to make a session stream, it is not necessary to reconstruct the packets which are fragmented, logfile can be analysed very easily. This feature is useful to log the comparatively large session such as telnet. Administrator can watch the telnet session of remote user as one stream unit until the connection close, if cracker makes telnet session to other network by way of administrated network, gdd can log all activities of cracker as one stream that includes other network. Furthermore, gdd have IDS function based on "grepmonitors session stream, if suspicious action is detected, gdd executes specified action.				
Hogwash for IPTables			http://www.prismnet.com/~aef/index2.html	2001
A modified version of Hogwash that integrates with Linux Netfilter/IPTables.				
Honeyd			http://www.citi.umich.edu/u/provos/honeyd/	2003
Honeyd is a small daemon that creates virtual hosts on a network. The hosts can be configured to run arbitrary services, and their personality can be adapted so that they appear to be running certain operating systems. Honeyd enables a single host to claim multiple addresses − I have tested up to 65536 − on a LAN for network simulation. Honeyd improves cyber security by providing mechanisms for threat detection and assessment. It also deters adversaries by hiding real systems in the middle of virtual systems.				
Hping	n/a		http://www.hping.org/	2002
hping is a command−line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and				

RAW−IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.				
httpcapture	n/a		http://www.steve.org.uk/Software/httpcapture/	2003
The tool designed here is a simple application which contains a couple of simple plugins for capturing, decoding, and displaying some network logins. Currently FTP/POP3/HTTP Basic Realms and CVS logins are supported.				
hunt	n/a		http://lin.fsid.cvut.cz/~kra/index.html#HUNT	2000
Hunt is a program for intruding into a connection, watching it and resetting it.				
idabench			http://idabench.ists.dartmouth.edu	2003
IDABench is an web interface to many intrusion analysis tools. By the use of simple plug−ins, it allows an analyst to twist and turn hourly packet logs through such utilities as tcpdump, ngrep, tethereal, etc. Output is textual web pages, gnuplot graphs, and downloadable composite binary dumpfiles. Based on the US Navy's SHADOW intrusion detection system, IDABench simplifies the writing of tcpdump filters, allows regular−expression context matching, and through a simple plugin API, can be extended to include other libpcap−based analysis tools, such as Snort, p0f, etc.				
iftop	n/a		http://www.ex−parrot.com/~pdw/iftop/	2003
iftop does for network usage what top(1) does for CPU usage. It listens to network traffic on a named interface and displays a table of current bandwidth usage by pairs of hosts.				
ip6sic			http://ip6sic.sourceforge.net/	2003
ip6sic is a tool for stress testing an IPv6 stack implementation.				
Ipaudit Ipaudit−web	−r	−w	http://ipaudit.sourceforge.net/ http://ipaudit.sourceforge.net/ipaudit−web/	2001
Ipaudit can summarize and/or log network activity down to the ip address and port level of detail, without recording every packet.				
Ipband	n/a		http://ipband.sourceforge.net/	2002
ipband is a pcap based IP traffic monitor. It tallies per−subnet traffic and bandwidth usage and starts detailed logging if specified threshold for the specific subnet is exceeded. If traffic has been high for a certain period of time, the report for that subnet is generated which can be appended to a file or e−mailed. When bandwidth usage drops below the threshold, detailed logging for the subnet is stopped and memory is freed.				
IPDump	*	n/a	http://sourceforge.net/projects/ipdump/	2000
IPdump is a tool to generate detailed packet header dumps from packet traces in LBNL's libpcap format. (* Default is to read pcap data from stdin)				
IPFM − IP Flow Monitor	−r	n/a	http://robert.cheramy.net/ipfm/	2002
IP Flow Meter is a bandwidth analysis tool, that measures how much bandwidth specified hosts use on their Internet link.				
IPgrab	−r	−w	http://ipgrab.sourceforge.net/	2002
IPgrab is a verbose packet sniffer for UNIX hosts.				
iplog	n/a		http://ojnk.sourceforge.net/	2001

iplog's capabilities include the ability to detect TCP port scans, TCP null scans, FIN scans, UDP and ICMP "smurf" attacks, bogus TCP flags (used by scanners to detect the operating system in use), TCP SYN scans, TCP "Xmas" scans, ICMP ping floods, UDP scans, and IP fragment attacks.				
IPPL − IP Protocols Logger			http://pltplp.net/ippl/	2000
ippl is a daemon which logs IP packets sent to a computer. It runs in the background, and displays information about the incoming packets.				
iptraf	n/a		http://cebu.mozcom.com/riker/iptraf	2002
IPTraf is a console−based network monitoring utility. IPTraf gathers data like TCP connection packet and byte counts, interface statistics and activity indicators, TCP/UDP traffic breakdowns, and LAN station packet and byte counts. IPTraf features include an IP traffic monitor which shows TCP flag information, packet and byte counts, ICMP details, OSPF packet types, and oversized IP packet warnings; interface statistics showing IP, TCP, UDP, ICMP, non−IP and other IP packet counts, IP checksum errors, interface activity and packet size counts; a TCP and UDP service monitor showing counts of incoming and outgoing packets for common TCP and UDP application ports, a LAN statistics module that discovers active hosts and displays statistics about their activity; TCP, UDP and other protocol display filters so you can view just the traffic you want; logging; support for Ethernet, FDDI, ISDN, SLIP, PPP, and loopback interfaces; and utilization of the built−in raw socket interface of the Linux kernel, so it can be used on a wide variety of supported network cards.				
ISIC			http://www.packetfactory.net/Projects/ISIC/	2000
ISIC is a suite of utilities to exercise the stability of an IP Stack and its component stacks (TCP, UDP, ICMP et. al.) It generates piles of pseudo random packets of the target protocol. The packets be given tendancies to conform to. Ie 50% of the packets generated can have IP Options. 25% of the packets can be IP fragments... But the percentages are arbitrary and most of the packet fields have a configurable tendancy. The packets are then sent against the target machine to either penetrate its firewall rules or find bugs in the IP stack. ISIC also contains a utility generate raw ether frames to examine hardware implementations.				
Jail	n/a		http://wiw.org/~ams/jail/	2001
jail (Just Another IP Logger) is a simple, but often useful network security tool which displays ICMP packets and attempted TCP connections from remote hosts.				
Kismet			http://www.kismetwireless.net/	
Kismet is an 802.11 wireless network sniffer − this is different from a normal network sniffer (such as Ethereal or tcpdump) because it separates and identifies different wireless networks in the area.				
Kripp			http://www.konst.org.ua/en/kripp	
KRIPP is a very simple and extremely light−weight network passwords sniffer written in Perl, which uses only the tcpdump utility as an underlying traffic interceptor. Can sniff and display ICQ, FTP, HTTP, CVS and POP3 passwords.				
Ksniffer			http://software.freshmeat.net/projects/ksniffer/	
KSniffer is a network statistics collector. It supports most TCP/IP protocols, (TCP, IP, UDP, ICMP, ARP, RARP as well as minimal IPX). Ksniffer reports on traffic in bytes or packets, activity (kbits/sec, kbytes/sec, packets/sec), as well as by protocol (http, irc, etc).				
LaBrea	n/a	 	http://www.hackbusters.net/LaBrea/ http://www.stearns.org/labrea/	2003

LaBrea is a program that creates a tarpit or, as some have called it, a "sticky honeypot". LaBrea takes over unused IP addresses on a network and creates "virtual machines" that answer to connection attempts. LaBrea answers those connection attempts in a way that causes the machine at the other end to get "stuck", sometimes for a very long time.				
lbrouter			http://www.qacafe.com/lbrouter/	
lbrouter is a test suite for Load Balancing and NAT related functionality. It verifies the operation of basic NAT, NAPT (port translation), and load balancing. It can also verify devices that support URL balancing and other related functions.				
Lcroex Rzobox			http://www.laurentconstantin.com/en/lcrzoex/ http://www.laurentconstantin.com/en/rzobox/	
Lcrzoex is a toolbox for network administrators and network hackers containing over 400 tools. These can perform network discovery, sniff the lan, check checksums, intercept sessions, check router configuration, determine if a firewall blocks specific protocols, and much more. RzoBox is a graphical front−end to lcrzoex.				
LFT − Layer Four Traceroute			http://www.mainnerve.com/lft/	
LFT, short for Layer Four Traceroute, is a sort of 'traceroute' that often works much faster (than the commonly−used Van Jacobson method) and goes through many configurations of packet−filter based firewalls. More importantly, LFT implements numerous other features including AS number lookups, loose source routing, netblock name lookups, et al.				
linsniff666	n/a		http://www.cotse.com/sw/sniffers/linsniff666.c	1999
linsniffer	n/a		http://www.phreak.org/archives/exploits/unix/network−sniffers/linsniffer.c	2001
linsniffer is simple sniffer whose main purpose is to capture usernames and passwords.				
lsrscan		? 	http://gaia.synacklabs.net/projects/lsrscan/	2003
lsrscan checks the behavior of remote hosts to loose source routed packets.				
lsrtunnel		? 	http://www.synacklabs.net/projects/lsrtunnel/	2003
lsrtunnel spoofs connections using source routed packets. lsrtunel will only be able to spoof connections against hosts that reverse source routed packets.				
Macsniffer			http://personalpages.tds.net/~brian_hill/macsniffer.html	2001
MacSniffer is a front end to the built−in 'tcpdump' packet sniffer on Mac OS X. MacSniffer allows you to view all of the traffic on a network connection, such as ethernet. MacSniffer includes a filter editing interface and a filter library to easily construct and reuse packet filters to view a subset of all the traffic on the connection, such as just that destined for a specific host or port. You can choose the level of detail you want captured, from just the minimal packet headers (showing source and destination hosts and ports) up to a full hex and ASCII dump of the packet contents.				
macwatch	n/a		http://mybox.trenger.ro/	2002
Small daemon to log activity from one or more devices (it does so by examining the packets that goes to and from the given MAC−adress, and reading the packet−length). I made it to monitor some servers on a DMZ and show how much bandwith they use with MRTG.				
Magic Lantern				

Mognet	n/a		http://www.chocobospore.org/projects/mognet/	2002
Mognet is a free, open source wireless ethernet sniffer/analyzer written in Java. It is licensed under the GNU General Public License. It was designed with handheld devices like the iPaq in mind, but will run just as well on a desktop or laptop.				
myNetMon			http://www.trsecurity.net/mynetmon/#1	
myNetMon is windows based network monitor and packet analyzing (sniffer) tool.				
Naimpass	−o	n/a	 http://www.nightfallsecurity.com/downloads/ndump.html	2000
Simple program that decodes aol instant messenger passwords from within an ndump output file.				
Nast		−l	 http://nast.berlios.de/	
Nast is a packet sniffer and a LAN analyzer based on Libnet and Libpcap. It can sniff in normal mode or in promiscuos mode the packets on a network interface and log it. It dumps the headers of packets and the payload in ascii or ascii−hex format. You can apply a filter. The sniffed data can be saved in a separated file.				
Ndump	n/a	−o	 http://www.nightfallsecurity.com/downloads/ndump.html	1999
ndump.pl dumps all packets on the network to a file in a raw data format.				
Nemesis	n/a		 http://www.packetfactory.net/projects/nemesis/ http://cerberus.sourcefire.com/~jeff/nemesis/	2003
Nemesis is a command−line UNIX libnet−based network packet injection suite.				
Nessus	n/a		 http://www.nessus.org/	2003
The "Nessus" Project aims to provide to the internet community a free, powerful, up−to−date and easy to use remote security scanner. A security scanner is a software which will audit remotely a given network and determine whether bad guys (aka 'crackers') may break into it, or misuse it in some way. Unlike many other security scanners, Nessus does not take anything for granted. That is, it will not consider that a given service is running on a fixed port − that is, if you run your web server on port 1234, Nessus will detect it and test its security. It will not make its security tests regarding the version number of the remote services, but will really attempt to exploit the vulnerability. Nessus is very fast, reliable and has a modular architecture that allows you to fit it to your needs.				
Netacct			 http://netacct−mysql.sourceforge.net/	2003
netacct−mysql is improved version of net−acct originally written by Ulrich Callmeier. This package logs network traffic. It provides a daemon (nacctd) that logs all traffic passing the machine it runs on (similiar to what mrta does). It supports peering file which means that you can divide you traffic in international and local peering.				
Netdude			 http://netdude.sourceforge.net/	
Netdude is the NETwork DUmp data Displayer and Editor for tcpdump tracefiles. It is a GUI−based tool that allows you to make detailed changes to packets in tcpdump tracefiles.				
Netfilter Ulogd module	n/a	*	 http://www.gnumonks.org/projects/ulogd	2003
ulogd is an universal logging daemon for the ULOG target of netfilter, the Linux 2.4 firewalling subsystem. ulogd is able to log packets in various formats to different targets (text files, databases, pcap, etc..). It has an easy−to−use plugin interface to add new protocols and new output targets. (* See pcapfile parameter.)				
Netl			 http://www.netl.org/netl/	2002

netl is a customizable low level network monitor. netl can be configured to look for particular TCP, UDP or ICMP packets, or can be setup to look for generic IP packets or even raw ethernet frames.				
Netstumbler			http://www.stumbler.net/	2003
Netstumbler is a Windows and PDA program (see Ministumbler) used to locate Wireless Access Points.				
Nettimer			http://mosquitonet.stanford.edu/~laik/projects/nettimer/	
Nettimer is a project to do end−to−end network performance measurement. It can listen passively to existing network traffic or actively probe the network. End−to−end means that we don't depend on any special information from the network and we don't depend on a particular transport protocol. The metric that we've currently implemented is bottleneck link bandwidth.				
Network Probe			http://www.objectplanet.com/probe/	2003
This network monitor and protocol analyzer gives you an instant picture of the traffic situation on your network and enables you to monitor network traffic in real time, hunt down, identify, and isolate traffic problems and congestions on your network. All traffic is monitored in real time and presented to the user as a combination of tables and charts, giving detailed information about hosts and protocols, as well as an instant overview of the traffic situation on your network.				
NetworkActiv PIAFCTM			http://www.networkactiv.com/PIAFCTM.html	
This can receive and analyze IP packets from your network or the internet, as well as collect packets of the HTTP protocol, analyze them, construct them into usable files, and then automatically save these files to a user specified directory.				
NetworkActiv scanner			http://www.networkactiv.com/Scanner.html	
This is a network exploration and administration tool. This tool can scan and explore internal LAN's and external WAN's. This tool is intended to be used by experienced network administrators and by novices.				
NFR − Network Flight Recorder			http://www.nfr.com/	
NFR Security provides a network intrusion management system that unobtrusively monitors your network in real−time, raises alerts when attacks or misuse are detected, actively responds if configured to do so, and integrates with popular firewalls to prevent future attacks.				
ngrep	−I	−O		http://ngrep.sourceforge.net/ http://www.stearns.org/doc/ngrep−intro.current.html	2001
Ngrep strives to provide most of GNU grep's common features, applying them to the network layer. ngrep is a pcap−aware tool that will allow you to specify extended regular expressions to match against data payloads of packets. It currently recognizes TCP and UDP across ethernet, ppp and slip interfaces, and understands bpf filter logic in the same fashion as more common packet sniffing tools, like tcpdump and snoop.				
Nitpicker	n/a			http://nitpicker.de/	2003
Nitpicker is an Ethernet accounting tool, which listens on an interface and accumulates all packets into flows. As it has been designed for *BSD's BPF, it also runs on Linux using libpcap. It writes raw file format flow files and has a dumping utility, and includes some tools for ISP billing.				
Nmap	n/a			http://www.insecure.org/nmap/index.html http://www.eeye.com/html/Research/Tools/nmapNT.html http://brianhill.dyndns.org/BetaStuff (MacNmap, OS X)	2003
Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP				

packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.					
Nparse	−o	n/a		http://www.nightfallsecurity.com/downloads/ndump.html	1999
Simple configurable parse script for ndump.pl output files. Prints out configured protocol headers in hex, ord, and bin and payload in ascii/hex. Currently it supports arp, ip, tcp, udp, icmp, rawip.					
Nprobe				http://www.ntop.org/nProbe.html	
nProbe is a NetFlow v5 Probe.					
NSAT − Network Security Analysis Tool		n/a		http://nsat.sourceforge.net/	2003
NSAT is a fast, highly configurable, bulk network security scanner for over 50 different services and hundreds of vulnerabilities.					
nstreams	−f	n/a		http://www.hsc.fr	
nstreams is a utility designed to identify the IP streams that are occuring on a network from a non−user friendly tcpdump output of several megabytes.					
ntop	−f	−l		http://www.ntop.org/ntop.html	2003
ntop is a network traffic probe that shows the network usage, similar to what the popular top Unix command does.					
Obfugator			? 	http://project.honeynet.org/tools/	2003
Obfugator can sanitize pcap capture files, both headers and payload.					
open1x			? 	http://www.open1x.org/	2003
IEEE 802.1x is a port based authentication protocol.					
p0f	−s	n/a		http://www.stearns.org/p0f/	2003
p0f performs passive OS fingerprinting technique based on information coming from remote hosts when they establish connections to our system. Captured packets contain enough information to determine OS − and, unlike active scanners (nmap, queSO) − it is done without sending anything to this host.					
Packet−httpd				http://www.bitwaste.com/projects/packet−httpd/	
packet−httpd is a test implementation of an httpd without a tcp/ip stack.					
Packet Monster				http://web.sfc.keio.ac.jp/~keiji/backup/ids/pakemon/	
pakemon has been developed to share IDS components based on the open source model. Current version of pakemon monitors all traffic on a network, search given data patterns in the traffic and output session logs and summary logs of matched traffic.					
PacketMon				http://www.analogx.com/contents/download/network/pmon.htm	
AnalogX PacketMon allows you to capture IP packets that pass through your network interface. Once the packet is received, you can use the built in viewer to examine the header as well as the contents or export the packets. PacketMon has a powerful rule system that allows you to narrow down the packets it captures to					

ensure you get exactly what you're after, without tons of unrelated information.					
Packetyzer				http://www.packetyzer.com/	
Packetyzer[tm] is a Windows user interface for the Ethereal packet capture and dissection library.					
packit	−r	−w		http://packit.sourceforge.net/	2003
Packit is a network auditing tool. Its value is derived from its ability to customize, inject, monitor, and manipulate IP traffic. By allowing you to define (spoof) nearly all TCP, UDP, ICMP, IP, ARP, RARP, and Ethernet header options, Packit can be useful in testing firewalls, intrusion detection/prevention systems, port scanning, simulating network traffic, and general TCP/IP auditing. Packit is also an excellent tool for learning TCP/IP.					
Pandora				http://www.nmrc.org/project/pandora/	
Pandora is a set of tools for hacking, intruding, and testing the security and insecurity of Novell Netware. It works on versions 4 and 5. Pandora consists of two distinct sets of programs −− an "online" version and an"offline" version. Pandora Online is intended to be used for direct attack against a live Netware 4 or 5 server. Pandora Offline is intended to be used for password cracking after you have obtained copies of NDS.					
pdumpq	n/a	*		http://rouxdoo.freeshell.org/dmn/pdumpq/	2001
Pdumpq takes packets over the netlink device which have been sent by Netfilter's QUEUE target and dumps them in Pcap format. This format is compatible with various packet sniffers such as tcpdump, snort and ethereal. (* Output file is last parameter on the command line.)					
Peep: The Network Auralizer				http://www.auralizer.com:8080/peep	2002
Peep is a network monitoring tool that represents network information via an audio interface. Network diagnostics are made not only based on single network events but whether the network sounds "normal".					
Petitmon				http://web.sfc.keio.ac.jp/~keiji/backup/ids/petitmon/	
petitmon is a simple network traffic recorder that generates a record of traffic on a connected wire in comma separated value(CSV) format.					
pktstat				http://www.itee.uq.edu.au/~leonard/personal/software/#pktstat http://www.stearns.org/pktstat/	2003
Display a real−time list of active connections seen on a network interface, and how much bandwidth is being used by what. Partially decodes HTTP and FTP protocols to show what filename is being transferred. X11 application names are also shown. Entries hang around on the screen for a few seconds so you can see what just happened. Also accepts filter expressions a la tcpdump.					
Promiscan	n/a			http://www.securityfriday.com/ToolDownload/PromiScan/promiscan_doc.html	2002
This software searches for promiscuous nodes on the local net.					
PSH − Packet SHell				http://playground.sun.com/psh/	1997
Packet Shell is an extensible Tcl/Tk based software toolset for protocol development and testing. It creates Tcl commands that allow you to create, modify, send, and receive packets on networks.					
ring		?		http://www.planb−security.net/wp/ring.html http://www.intranode.com/fr/doc/ring−full−paper.pdf	
By measuring the behavior of various operating systems' TCP retransmission timeout lengths (or RTOs), it is possible to distinguish between OSes on a network. Franck Veysset, Olivier Courtay, and Olivier Heen of the					

Intranode Research Team first published this concept in April, 2002, and their paper goes into appreciable detail in its discussion of this technique, the mechanisms by which TCP retransmission timers are computed, and OS fingerprinting in general. To demonstrate this concept, the researchers simultaneously released a proof−of−concept tool which leverages this specific exposure: Remote Identification, Next Generation, or RING.				
Rpcap			http://rpcap.sourceforge.net/	2002
RPCAP is a Remote Packet Capture system. It enables you to run a packet capture program (the server) on a target computer, which will sniff the network traffic on that system, and uplink the captured packets to another host (the client), where the captured packets can be processed, analysed and archived.				
rtdump	−r	−w	http://rpcap.sourceforge.net/	2002
Rtdump is a version of tcpdump modified to capture traffic on remote systems and networks. It links to librpcap rather than libpcap. Apart from the additional requirments introduced by the remote capture paradigm, rtdump is identical to tcpdump in command syntax and use.				
Scanlogd	n/a		http://www.fatsquirrel.org/veghead/software/	1999
Solar Designer's excellent tool for detecting port scans, now hacked into supporting libpcap.				
Sendip			http://www.earth.li/projectpurple/progs/sendip.html	2003
SendIP is a commandline tool to allow sending arbitrary IP packets.				
Sentinel	n/a		http://www.packetfactory.net/projects/sentinel/	2001
The sentinel project is an implementation of effective remote promiscuous detection techniques.				
Shadow			http://www.nswc.navy.mil/wwwDL/XD/ISSEC/CID/	2003
Shadow is an Intrusion Detection system based on inexpensive PC hardware running Open Source, public domain, or freely available software components. A Shadow system consists of at least two pieces: a sensor located at a point near an organization's firewall, and an analyzer located inside the firewall.				
SING			http://sourceforge.net/projects/sing/	2001
SING stands for 'Send ICMP Nasty Garbage'. It is a tool that sends ICMP packets fully customized from the command line. Its main purpose is to replace the ping command but adding certain enhancements (Fragmentation, spoofing...)				
Siphon	n/a		http://siphon.datanerds.net/	2000
The Siphon Project is a portable passive network mapping suite. In the latest public version, Siphon passively maps TCP ports and performs passive operating system detection.				
snacktime		? 	http://www.plan9−security.net/wp/snacktime.html	2003
Franck Veysset, Olivier Courtay, and Olivier Heen of Intranode research noticed that one could fairly reliably detect a wide range of operating systems by timing the retransmission timeout lengths of the TCP handshake. Turns out, this is not only a surprisingly reliable, but has the potential to be extremely stealthy. Being that I'm a chimp, I'm much better with Perl than I am with C, so I ported the concepts over, and added on some extra passive fingerprinting techniques. The result is Snacktime −− a half−open, half−passive OS Fingerprinting tool.				
Sniffer			http://stev.org/sniffer.html	2001

Features: an ncurses user interface, network statistics to view the amount of packets and data in man different protocols and by interface, view what active TCP connections are on the network, view UDP and ICMP packets, view and log the 48bit arp protocol, multithreaded so that the user interface does not interfere with any of the packet capturing methods, and view and log the following user space protocols: FTP, POP3, HTTP.					
Sniffit	−r	−R		http://reptile.rug.ac.be/~coder/sniffit/sniffit.html	1998
sniffit is a packet sniffer for TCP/UDP/ICMP packets. sniffit is able to give you very detailed technical info on these packets (SEQ, ACK, TTL, Window, ...) but also packet contents in different formats (hex or plain text, ...).					
Sniffit/win2k				http://www.symbolic.it/Prodotti/sniffit.html	2000
Sniphere				http://www.securesphere.net/html/projects_sniphere.php	
Sniphere is a network sniffer that supports most common protocols.					
Snmpsniff				http://elektra.porto.ucp.pt/snmpsniff/	
SnmpSniff is a promiscuous SNMP PDU sniffer. Because it is dedicated to the SNMP protocol, it offers exhaustive analysis of its packets. I recommend it for anyone analyzing SNMP transactions, and for anyone involved in teaching or instruction about network management.					
Snoop	−i	−o		http://www.spitzner.net/snoop.html	
Snoop is a network sniffer packaged with Solaris.					
Snoopanalyzer				http://www.snoopanalyzer.com/	
SnoopAnalyzer Professional is a network protocol analyzer based on network data capturing technology under Microsoft Windows platforms(95/98/Me/2000NT/XP). SnoopAnalyzer Professional includes ARP spoofing.					
Snort	−r	−b		http://www.snort.org	2003
Snort is a libpcap−based packet sniffer/logger which can be used as a lightweight network intrusion detection system. It features rules based logging and can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort has a real−time alerting capabilty, with alerts being sent to syslog, a seperate "alert" file, or as a WinPopup message via Samba's smbclient					
SPIE − Source Path Isolation Engine				http://www.net−tech.bbn.com/projects/SPIE/	
BBN Technologies is developing the Source Path Isolation Engine (SPIE), a hash−based technique for IP traceback that generates audit trails for traffic within a network. The audit trails are used to trace the origin of any single packet delivered by the network in the recent past.					
stegtunnel		?		http://www.synacklabs.net/projects/stegtunnel/	2003
Stegtunnel provides a covert channel in the IPID and sequence number fields of any desired TCP connection. It requires the server and client to have a previously shared secret in common to detect and decrypt the data. You don't have to worry about the connections looking unlike real TCP connections, because they are real connections, just with extra info in certain fields.					

Tcpdpriv	−r	−w		http://ita.ee.lbl.gov/html/contrib/tcpdpriv.html	1997
Tcpdpriv is program for eliminating confidential information from packets collected on a network interface (or, from trace files created using the −w argument to tcpdump).					
Tcpdstat	*	n/a		http://staff.washington.edu/dittrich/talks/core02/tools/tools.html	2002
Produces a per−protocol breakdown of traffic by bytes and packets, with average and maximum transfer rates, for a given libpcap file (e.g., from tcpdump, ethereal, snort, etc.) Useful for getting a high−level view of traffic patterns. (* Input file is the last parameter on the command line.)					
Tcpdump	−r	−w		http://www.tcpdump.org	
Tcpdump is a command−line tool for monitoring network traffic. Tcpdump can capture and display the packet headers on a particular network interface or on all interfaces. Tcpdump can display all of the packet headers, or just the ones that match particular criteria.					
Tcpflow				http://www.circlemud.org/~jelson/software/tcpflow/	
tcpflow is a program that captures data transmitted as part of TCP connections (flows), and stores the data in a way that is convenient for protocol analysis or debugging. A program like 'tcpdump' shows a summary of packets seen on the wire, but usually doesn't store the data that's actually being transmitted. In contrast, tcpflow reconstructs the actual data streams and stores each flow in a separate file for later analysis.					
TCPKillNT				http://members.fortunecity.com/sektorsecurity/projects/tcpkillnt.html	2001
TCPKillNT is a TCP connection "Reset" utility for Microsoft Windows NT platforms. It has the ability to send RST packets to already established TCP connections. Quite deadly on a LAN. It is very useful for IDS kind of products which need to terminate a TCP session. Requires Winpcap and LibnetNT.					
Tcpreplay	*	n/a		http://tcpreplay.sourceforge.net/	2003
tcpreplay is a BSD−style licensed tool to replay saved tcpdump files at arbitrary speeds. It provides a variety of features for replaying traffic for both passive sniffer devices as well as inline devices such as routers, firewalls, and the new class of inline IDS's. tcpreplay includes the following tools: tcpreplay, which replays capture files, tcpprep, a capture file pre−processor for creating cache files for tcpreplay, capinfo, which prints statistics about capture files, pcapmerge, a tool for merging pcap files into one larger one, and flowreplay, a tool for replaying connections. (* File(s) to read are the last parameter(s) on the command line.)					
tcpslice	*	−w		http://www.tcpdump.org	
Tcpslice is a program for extracting portions of packet−trace files generated using tcpdump's −w flag. It can also be used to glue together several such files. (* Files to read are the last parameters on the command line.)					
Tcpstat	−r	n/a		http://www.frenchfries.net/paul/tcpstat/	2003
tcpstat reports certain network interface statistics much like vmstat does for system statistics. tcpstat gets its information by either monitoring a specific interface, or by reading previously saved tcpdump data from a file.					
Tcptrace				http://www.tcptrace.org/	
tcptrace is a tool written by Shawn Ostermann at Ohio University, for analysis of TCP dump files. It can take as input the files produced by several popular packet−capture programs, including tcpdump, snoop, etherpeek, HP Net Metrix, and WinDump. tcptrace can produce several different types of output containing information on each connection seen, such as elapsed time, bytes and segments sent and recieved, retransmissions, round trip times, window advertisements, throughput, and more. It can also produce a					

number of graphs for further analysis.				
Tcptraceroute	n/a		http://michael.toren.net/code/tcptraceroute/	2003
tcptraceroute is a traceroute implementation using TCP packets. By sending out TCP SYN packets instead of UDP or ICMP ECHO packets, tcptraceroute is able to bypass the most common firewall filters.				
Tcpurify	−f	−o		http://masaka.cs.ohiou.edu/~eblanton/tcpurify/	2002
TCPurify is a packet sniffer/capture program similar to tcpdump, but with much reduced functionality. What sets TCPurify apart from other, similar programs is its focus on privacy. TCPurify is designed from the ground up to protect the privacy of users on the sniffed network as much as possible. In order to accomplish this goal, TCPurify truncates almost all packets immediately after the last recognized header (IP or Ethernet), removing all data payload before storing the packet. Furthermore, it has the capability of randomizing some or all IP addresses (based on the network portion of the address) to mask exactly where packets are where or to while still retaining some general idea.				
Tracelook				http://www.cs.helsinki.fi/u/gurtov/win−tracelook/	
This is the all−in−one package for displaying traces in binary tcpdump format (recorded with −w option) for Windows. It includes tracelook, windump, txgraph, tcl/tk, and awk. It does not require cygwin or anything else to operate. It works at least in Windows 98/NT/2k.				
ttlscan		? 	http://raisdorf.net/?page=projects/td>	2003
ttlscan is a libnet/libpcap based program that sends a TCP SYN packet to each port of the host given via the command line. The answer is sniffed of the wire. I use it to detect hosts that fake services by forwarding packets to another host (behind a firewall). By reading header files like the TTL, window size and IPID you might be able to see the OS running on the host behind the firewall. As of now it doesn't do anything useful but printing the ttl.				
User−Mode Linux			http://user−mode−linux.sourceforge.net/networking.html	2003
User−Mode Linux gives you a virtual machine that may have more hardware and software virtual resources than your actual, physical computer. The pcap transport is a synthetic read−only interface, using the libpcap binary to collect packets from interfaces on the host and filter them. This is useful for building preconfigured traffic monitors or sniffers.				
VTA − Visual tcp /udp Animator			http://cs.mtu.edu/vta/	
VTA displays packets captured from the network in any of several views that, when used individually or in combination, help to depict operation of the TCP and UDP protocols.				
Wellenreiter			http://www.remote−exploit.org/	2003
Wellenreiter is a wireless network discovery and auditing tool. Prism2, Lucent, and Cisco based cards are supported. It can discover networks (BSS/IBSS), and detects ESSID broadcasting or non−broadcasting networks and their WEP capabilities and the manufacturer automatically.				
Wifiscanner	n/a	−W		http://wifiscanner.sourceforge.net/	2003
WifiScanner is an analyzer and detector of 802.11b stations and access points. It can listen alternatively on all the 14 channels, write packet information in real time, can search access points and associated client stations, and can generate a graphic of the architecture using GraphViz. All network traffic can be saved in the libpcap format for post analysis. It works under Linux with a PrismII card and with the linux−wlan driver.				

Windump	−r	−w		http://windump.polito.it/	2002
WinDump is the porting to the Windows platform of tcpdump, the most used network sniffer/analyzer for UNIX. Porting is currently based on version 3.5.2. WinDump is fully compatible with tcpdump and can be used to watch and diagnose network traffic according to various complex rules. It can run under Windows 95/98/ME, and under Windows NT/2000/XP.					
Xprobe				http://www.sys−security.com/html/projects/X.html	
Xprobe is an Active OS fingerprinting tool based on Ofir Arkin's ICMP Usage In Scanning Research project. Xprobe is an alternative to some tools which are heavily dependent upon the usage of the TCP protocol for remote active operating system fingerprinting.					
ZX SNiffer				http://bazzar.com.ua/?z=portfolio.win	
Shows network traffic: ICMP, IGMP, UDP, TCP. Intercepts and decodes passwords of: POP3, FTP, ICQ, Basic Proxy and Web Authorization.					
Libraries					
Billy the Kid	n/a	Python		http://home.student.utwente.nl/g.v.berg/btk/	
Billy the Kid is a Python Extension Module providing you with all kinds of more or less usefull stuff at the raw packet level. It allows you to create raw UDP/TCP/ICMP packets and it also includes a nice interface to libpcap.					
Jpcap	n/a	Java		http://netresearch.ics.uci.edu/kfujii/jpcap/doc/	
Jpcap is a Java class package which enables to capture and send IP packets from Java application. This package uses libpcap / winpcap and Raw Socket API.					
libdnet	n/a			http://libdnet.sourceforge.net/	2003
libdnet provides a simplified, portable interface to several low−level networking routines, including network address manipulation, kernel arp(4) cache and route(4) table lookup and manipulation, network firewalling (IP filter, ipfw, ipchains, pf, ...), network interface lookup and manipulation, and raw IP packet and Ethernet frame transmission.					
libnet	n/a			http://www.packetfactory.net/libnet/ http://linbnet.sourceforge.net − old?	
Libnet is an API to help with the construction and handling of network packets. It provides a portable framework for low−level network packet writing and handling (use libnet in conjunction with libpcap and you can write some really cool stuff). Libnet includes packet creation at the IP layer and at the link layer as well as a host of supplementary and complementary functionalty. Libnet is avery handy with which to write network tools and network test code.					
Libnet/win32	n/a			http://utenti.lycos.it/webteca/libnet.htm	
Libnet is a high−level API (toolkit) allowing the application programmer to construct and inject network packets. It provides a portable and simplified interface for low−level network packet shaping, handling and injection.					
Libnetnt	n/a			http://www.eeye.com/html/Research/Tools/libnetnt.html	2000
LibnetNT has the exact same functionality and abilities as Libnet, and LibnetNT can be used to develop low−level packet injection programs on Windows NT 4.0 and Windows NT 5.0. LibnetNT has been encapsulated in a dll file so users can call the Libnet functions from almost any Windows NT programming language (i.e. you could write a SYN flooder in Visual Basic).					

libpcap	n/a		http://www.tcpdump.org	
Libpcap provides a portable framework for low−level network monitoring. Libpcap can provide network statistics collection, security monitoring and network debugging. Since almost every system vendor provides a different interface for packet capture, the libpcap authors created this system−independent API to ease in porting and to alleviate the need for several system−dependent packet capture modules in each application.				
Net::Pcap	n/a	Perl	http://search.cpan.org/author/KCARNUT/Net−Pcap−0.05/Pcap.pm	
Net::Pcap is a Perl binding to the LBL pcap(3) library, version 0.7.2.				
Net::Pcap for Win32	n/a	Perl 	http://www.bribes.org/perl/wnetpcap.html	
A port of the Perl Net::Pcap module to Win32.				
Net::RawIP	n/a	Perl	http://quake.skif.net/RawIP/	
NetRawIP is a Perl extension for manipulating raw IP packets. It includes an interface to Libpcap. This package provides a class object that can be used to create, manipulate and send raw IP packets and manipulate Ethernet headers				
NetPacket	n/a	Perl	http://cpan.org/authors/id/T/TI/TIMPOTTER/	
These Perl modules do basic disassembly of network packets of various Internet protocols, and contain hooks for assembly of packets.				
py−libpcap py−libpcap−win32	n/a	Python 	http://sourceforge.net/projects/pylibpcap/ http://www.ghaering.de/python/unsupported/pylibpcap/	
Python module for the libpcap packet capture library, based on the original python libpcap module by Aaron Rhodes.				
pycap	n/a	Python	http://pycap.sourceforge.net/	2003
PyCap is a high−level Python interface to the libpcap packet capture library. It can parse the raw packet data into easily accessible Python objects representing Ethernet, IP, UDP, TCP, and ICMP headers.				
pynetlibs	n/a	Python	http://pynetlibs.sourceforge.net/default.html	2002
py_net_libs are a collection of functions to decode network data as return by pylibpcap.				
Ruby/pcap extension library	n/a	Ruby	http://www.goto.info.waseda.ac.jp/~fukusima/ruby/pcap−e.html	
Ruby interface to LBL Packet Capture library. This library also includes classes to access packet header fields.				
Winpcap	n/a		http://winpcap.polito.it/	
WinPcap is an architecture for packet capture and network analysis for the Win32 platforms. It includes a kernel−level packet filter, a low−level dynamic link library (packet.dll), and a high−level and system−independent library (wpcap.dll, based on libpcap version 0.6.2). It's available for Windows 95, 98, ME, NT, 2000, and XP.				
Supporting tools				
GNUPlot	n/a		http://www.gnuplot.info	
gnuplot is a command−driven interactive function plotting program. It can be used to plot functions and data points in both two− and three−dimensional plots in many different formats, and will accommodate many of the needs of today's scientists for graphic data representation. gnuplot is copyrighted, but freely distributable; you don't have to pay for it. If available, IDABench will use it to produce graphs.				

Additional Sniffer indexes:

- http://www.insecure.org/tools.html
- http://www.geocities.com/sk8colio/packetsniffer.html
- http://www.antioffline.com/TID/sniffers/
- http://www.tcpdump.org/related.html
- http://winpcap.polito.it/misc/links.htm
- http://www.solaris4you.dk/sniffersSS.html
- http://dachb0den.com/archives/tools.html
- http://www.l0t3k.org/security/tools/sniffing/
- http://www.webattack.com/Freeware/network/fwpacketsniffer.shtml
- http://home.wanadoo.nl/hackjegek/sniffing.htm
- http://packetstormsecurity.nl/sniffers/
- http://www.mycert.org.my/resource/ids.htm
- http://www.pakcert.org/ids.html
- http://www.cotse.com/tools/sniffers.htm
- http://rak.isternet.sk/linux−netman/monitoring.html
- http://www.ozetechnology.com/goodies/Networking.shtml
- http://www.robertgraham.com/pubs/sniffing−faq.html
- http://www.securityfocus.com/tools/category/4
- http://www.phreak.org/archives/exploits/unix/network−sniffers/
- http://www.unixgeeks.org/security/newbie/security/sniffer/sniffer.html
- http://freshmeat.net/search/?q=libpcap
- http://www.mirrors.wiretapped.net/security/packet−capture/
- http://security.royans.net/projects/pentest/
- http://libdnet.sourceforge.net/

Tutorials

- http://www.cet.nau.edu/~mc8/Socket/Tutorials/section1.html
- http://www.ethermanage.com/ethernet/ethernet.html
- http://www.linux4biz.net/articles/articlesniff.htm
- http://www.boran.com/security/sniff.html (1995)
- http://www.unixgeeks.org/security/newbie/security/sniffer/sniffer.html
- http://www.linuxjournal.com/article.php?sid=5201
- http://www.tcpdump.org/pcap.htm
- http://www.ironcomet.com/sniffer.htm
- http://www.packet−level.com/
- http://www.whitehats.ca/main/members/Malik/malik_tcpdump_filters/malik_tcpdump_filters.html
- http://www.alphalink.com.au/~tjaden/libnet−HOWTO/

Pcap sample files

- http://www.shmoo.com/cctf/
- http://project.honeynet.org/misc/chall.html
- http://project.honeynet.org/scans/
- http://www.packet−level.com/traceFiles.htm
- http://project.honeynet.org/papers/forensics/exploit.html
- http://www.stearns.org/pcap/
- http://project.honeynet.org/misc/files/data−demo.tgz

- http://ita.ee.lbl.gov/html/traces.html
- http://tracer.csl.sony.co.jp/mawi/
- http://www.cs.columbia.edu/~hgs/internet/traces.html

William is an Open−Source developer, enthusiast, and advocate from New Hampshire, USA. His day job at SANS pays him to work on network security and Linux projects.

Last updated 12/5/2003.